العنوان:	المعلوماتية والمسؤولية الجزائية
المصدر:	مجلة الفكر الشرطي - مركز بحوث الشرطة - القيادة العامة لشرطة الشارقة - الإمارات
المؤلف الرئيسي:	مصطفي، خالد حامد أحمد
المجلد/العدد:	مج20, ع79
محكمة:	نعم
التاريخ الميلادي:	2011
الشهر:	أكتوبر
الصفحات:	147 - 185
رقم MD:	605747
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	HumanIndex
مواضيع:	المعلوماتية
رابط:	http://search.mandumah.com/Record/605747

المعلوماتية والمسؤولية الجزائية (1)

الدكتور خالد حامد أحمد مصطفى (2)

أستاذ مساعد بقسم القانون الجنائي – كلية القانون
جامعة عجمان – الإمارات العربية المتحدة

مستخلص

تهدف هذه الدراسة إلى التعرف على جرائم المعلومات ـ باعتبارها تضم كافة أنماط السلوك الإجرامي العمدي أو غير العمدي التي تقع في مجال المعلومات ـ وبالرغم من استخدام نظرية متكاملة في تفسير جرائم المعلومات وكافة صورها وأنواعها إلا أن النصوص العقابية في أغلب التشريعات لا تتلاءم مع الفكر العقابي الحديث وخلصت هذه الدراسة إلى تقسيم جرائم المعلومات إلى أربعة أنواع رئيسية ، الأولى جرائم الحاسب الآلي. والثاني شبكة الإنترنت. والثالث شبكة الإنترنت المصرفية. والرابع الأقمار الصناعية. وأوضحت وجود نزاع تشريعي انعكس على ضبط السلوك الإجرامي لهذه الجرائم ، حيث وجدت بعض المشاكل والصعوبات تتعلق في الجهة المختصة بإجراءات الاستدلال والتحقيق حيث تتعلق هذه الجرائم بمعلومات وبيانات وشبكة اتصال تتواجد في عدة أماكن أو دول مما يجعلها تختلف عن الجرائم التقليدية كما أوضحت الدراسة أيضاً أن هناك صعوبات تثور في مرحلة المحاكمة فيما يتعلق بدلائل إثبات الجريمة ومقوماته ولا سيما أنه في محيط جرائم المعلومات لا يستطيع القاضي تطبيق إجراءات الإثبات التقليدية كما يثور أيضاً تساؤلات تتعلق بمشكلة إقليمية القانون وما هو القانون الواجب التطبيق على الجرائم التي ترتكب في أكثر من دولة فهذه الجرائم تعد من الجرائم عابرة الحدود الإقليمية للدولة الأمر الذي يقتضي أن يكون هناك اتفاقات دولية بشأن تسليم المجرمين. ونادت الدراسة بضرورة تدريب موظفي إنفاذ القانون من قضاة ونيابة وشرطة على طرق ضبط ومكافحة الجرائم المعلوماتية وأوصت بضرورة إعادة صياغة النصوص العقابية بالشكل الذي يتلاءم مع الفكر العقابي الحديث لتشمل أكبر قدر من الجرائم مثل جرائم التعدي على حقوق شركات البث الإعلامي عبر الأقمار الصناعية أو استغلال هذه الأقمار الصناعية في أغراض التجسس الصناعي والاقتصادي والعسكري كما نادت الدراسة بضرورة التزام الدول بوضع ضوابط دولية للتعاون الدولي لمكافحة جرائم التعدي على المعلومات كما ينبغي على تشريعات الدول العربية الاقتداء بالتشريع الفرنسي الذي وضع ضوابط تكفل الحماية الجنائية ضد جرائم الإهمال في الحفاظ على البيانات وكذلك ضد جرائم سرقة بطاقات الائتمان كما نادت الدراسة أيضاً بضرورة تطوير نظم آمنة للتجارة الإلكترونية فضلاً عن ضرورة إنشاء قضاء متخصص من أعضاء النيابة وخبراء وقضاة النظر في جرائم المعلومات

مفردات البحث :

المعلوماتية – المسؤولية الجزائية – الجرائم المستحدثة – جرائم تقنية المعلومات – جرائم الحاسب الآلي – جرائم شبكة الإنترنت – جرائم الأقمار الصناعية.

1- ورد هذا البحث للدورية في يونيو 2011م وأحيل للتحكيم في يوليو 2011م وأجيز للنشر في أغسطس 2011م.

2- حصل الدكتور خالد حامد مصطفى على درجة الدكتوراه في القانون وسبق له العمل رئيس نيابة عامة وقاضياً ورئيس محكمة بجمهورية مصر العربية والباحث لديه مؤلف كتاب في الإجراءات الجزائية لدولة الإمارات العربية المتحدة كما أنه له العديد من البحوث والدراسات الأكاديمية وشارك في مؤتمرات وندوات محلية ودولية.

مقدمة :

يعد التقدم في تكنولوجيا المعلومات من أبرز التطورات العالمية المعاصرة ، حيث تلعب دوراً بارزاً في مجال البحث العلمي ، وكان من أبرز آلياتها أربعة محاور رئيسية **أولهما الحاسب الآلي** الذي ساهم بدوره في تعميق التعاون في نطاق تبادل المعلومات بين الدول والأفراد في مختلف المجالات ، ذلك أنه ببساطة شديدة "جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال المعلومات (data input) وإخراج المعلومات (information output) وإجراء عمليات حسابية ، كما ينطوي على برنامج الكتابة (word) حيث يتم حفظ الكتابة على وسائط تخزين ويتم استرجاعها من خلال مشغل النظام عن طريق لوحة المفاتيح ، ومعالجتها بعد ذلك بواسطة وحدة المعالجة المركزية (C.P.U) ، لكي يتسنى للمستخدم استخدام هذه الوسائط واسترجاعها وطباعتها [1].

ثانيهما شبكة (Internet) وهي شبكة عالمية ضخمة تربط هذه الأجهزة بعضها ببعض تسمى (Internet) وهذه الشبكة تحدث نوعاً من الربط بين أجهزة الحاسب الآلي في مختلف أنحاء العالم ، إضافة إلى أنها تستخدم في الاتصال الدولي ، وهي لا تخضع لملكية فرد معين ، أو دولة معينة ، وإنما تعمل من خلال بروتوكول بيانات المستخدم (User Datagram Protocol) ، وهي مجموعة من بروتوكولات الشبكات التي تستخدم للإنترنت ، يستطيع المستخدم بواسطتها نقل الرسائل والتي تعرف أحياناً بوحدة البيانات (Datagram) إلى أجهزة أخرى على شبكة تعمل ببروتوكول الإنترنت ، وذلك دون الحاجة إلى إجراء اتصالات أولية لإنشاء قنوات اتصال قبل بدء إرسال البيانات [2].

---

[1]- د. علاء الدين محمد فهمي ، الموسوعة الشاملة لمصطلحات الحاسب الآلي ، موسوعة دلتا كمبيوتر ، مطابع الكتاب المصري الحديثة ، 1991 ، ص 108.

[2]- http:www.orienttel.net.

كما تعد هذه الشبكة العالمية وسيلة اتصال أساسية بين الأفراد من خلال إرسال وتلقي الرسائل بواسطة خدمة البريد الإلكتروني ، كما تعطي ميزة للمستخدم من خلال التصفح الإلكتروني ، والتسوق والتجارة الإلكترونية ، وذلك لانخفاض تكاليف النقل (1).

ثالثهما شبكة الإنترنت المصرفية التي تسمح لعملاء البنوك بالبيع ، والشراء باستخدام وسائل الدفع البديلة للنقود مثل بطاقات الائتمان ، البطاقات البلاستيكية ، ووسائل الدفع الإلكترونية ، التي تتيحها البنوك وهي عبارة عن " بطاقات إلكترونية تحتوي على مخزون نقدي تصلح كوسيلة للدفع ، وأداة للإبراء ، ووسيطاً للتبادل ، وتقوم بغالبية الوظائف التي تقوم بها النقود الورقية حتى بات من المتوقع أن تحل هذه النقود الحديثة محل النقود على المدى الطويل " (2). **أخيراً الأقمار الصناعية** التي تمتلكها الدول وتستغلها في كافة الأغراض سواء البث الإعلامي للبرامج المختلفة ، أو في أغراض البحث العلمي ، أو مختلف الأغراض التي تخدم الدولة الإلكترونية.

وإذا كانت هــذه التطورات الهائلة ساهمت في تقدم العديد من المنافع ، والمزايا للدول ، والأفراد ، والكيانات الخاصة في شتى المجالات ، إلا أنه على الرغم من ذلك فقد نجم عنها مخاطر تتمثل في التعدي على هذه المحاور الأساسية ، أو استغلالها بشكل غير مشروع وهو ما يمكن تسميته بالجرائم المعلوماتية (3).

لذلك فإنه من الأهمية بمكان في هذه الورقة السعي للوقوف على تحديد معنى هذه الجرائم ، وأنواعها المختلفة ، وأشكالها الجديدة ، وذلك في إطار تلك التطورات العالمية

1- BernetRollanoe: L Principes de technique bancaire, Paris, Dunod, 2002, p 10.

2- Strategy Report- International Narcotics Control Released by the Bureau for International Narcotics and Law Enforcement Affairs -March 2004 http://www.state.gov/p/inl/rls/nrcrpt/2003/vol2/html/29910.htm

3- UNCTAD (2004), The E-Commerce and Development Report 2004, United Nations, New York and Geneva.

المعاصرة ، بهدف تحديد المخاطر المترتبة عليها ، ومن ثم تسهيل مهام الجهات الرسمية في تحديد واقتراح الوسائل والآليات المناسبة لمكافحتها.

مشكلة الدراسة :

أوضحنا حقيقة هامة وهي أن المعلومات باتت في عصرنا الحالي تشكل أهمية خاصة بسبب التقنيات المتطورة في تكنولوجيا المعلومات ، ولعبت شبكة الاتصالات الدولية دوراً رئيسياً في هذا التطور ، ولا سيما في ظل تنامي التجارة الإلكترونية وتسابق دول العالم المتطور نحو استخدام التجارة الإلكترونية بشكل واسع ، حيث تبين أحدث الأرقام تطور التجارة عالمياً ، ففي عام 1995 كان حجم التجارة الإلكترونية صفراً بالمائة ، وتطورت عام 1997 لتصل إلى 26 مليار دولار.

وقد استفادت الحكومات أيضاً من تلك التطورات بحيث أصبحت تمتلك القدرة على التعامل إلكترونياً وتقديم العديد من خدماتها من خلال الاتصال المباشر on-line ، الأمر الذي أدى في النهاية إلى ظهور ما يسمى بالحكومة الإلكترونية التي " تستغل تكنولوجيا المعلومات والاتصالات لتطوير وتحسين تدبير الشؤون العامة ، وذلك لإنجاز الخدمات الحكومية الرسمية بين الجهات الحكومية والمتعاملين معها ، بطريقة معلوماتية تعتمد على الإنترنت ، وفق ضمانات أمنية معينة تحمي المستفيد والجهة صاحبة الخدمة " [(1)].

لذلك كان من الأهمية بمكان وضع منظومة شاملة تكفل الحماية الجنائية الموضوعية والإجرائية ، بل والدولية ضد جرائم المعلومات ، وأشكالها وأنماطها المستحدثة ، ويجب أن يكون للفقه والباحثين دور هام في هذا الصدد ، حيث أن جرائم المعلومات أصبحت تهدد بشكل ملحوظ كافة مناحي الحياة ذلك من خلال الآتي :

- ضـــرورة حماية أجهزة الحاسوب وما تحتويه من محتوى معنوي كالمعلومات الهامة ، والأفكار ، والممتلكات من خلال قوانين تكفل التصدي لكافة أنماط هذه

[1]– المستشار الدكتور/ عبدالفتاح مراد ، الحكومة الإلكترونية ، مطبعة جامعة الإسكندرية ، ص 23.

الجرائم ، وتتلافى بعض الثغرات التشريعية في الدول التي تتناول بالتجريم جرائم تقنية المعلومات.

- ضمان شبكة الاتصال الدولية (Internet) ذلك لأن التعرض لها سواء بالتخريب أو وقفها أصبح أمراً بالغ الخطورة لأنه/ يهدد التجارة الإلكترونية/ والحريات الأساسية للأفراد في الاتصال ، والتعبير عن الرأي ، ولعل الأحداث التي شهدتها بعض الدول مؤخراً من قطع خدمات الإنترنت ، أو التعدي على حقوق الشركات التي تبث برامج تخضع لحماية خاصة لا يستفيد منها إلا المشتركون دليلاً على عدم وجود حماية لهذه الشبكات من التعدي عليها.
- بسط الحماية على الوسائل ، والآليات المرتبطة بأجهزة الحاسوب وأبرزها شبكة الإنترنت المصرفية المتعلقة بالبنوك ، وذلك للحيلولة دون استغلال بطاقات الائتمان المزورة ، أو المسروقة في سرقة أموال العملاء.
- التوسع في مدلول جرائم المعلومات لتشمل أنماطاً جديدة من الجرائم تعتمد على التطورات التكنولوجية الحديثة مثل التجسس العسكري والاقتصادي عبر الأقمار الصناعية ، وهو ما يحتاج إلى تضافر جهود المجتمع الدولي لما يمثله هذا النمط من الجرائم من طابع دولي.
- ضرورة وضع منظومة تشريعية متكاملة كأساس لتجريم الجرائم المستحدثة ، حيث أن بعض الجرائم المستحدثة وأبرزها جرائم المعلومات تحتاج إلى نصوص متميزة فأغلب الدول لا تتناول بالتجريم الأفعال غير العمدية في جرائم المعلومات.
- وضع منظومة إجرائية تبدأ من تحديد القانون الواجب التطبيق في جرائم المعلومات والمحكمة المختصة ، لما تمثله هذه الجريمة من صعوبات في أنها جريمة عابرة للحدود ، تحديد دور الجهة المختصة بالاستدلال ، والضبط ، والتفتيش وسلطتها في هذا الصدد ، والدليل المعلوماتي في الجريمة ومقوماته ، ومدى سلطة المحكمة بشأنه إذ لا يعقل أننا مازلنا نتعامل مع هذه الجرائم من خلال القوانين الإجرائية وهي لا تتلاءم بطبيعة الحال مع الجرائم المستحدثة.

ومن هنا يجدر بنا في هذا البحث أن نتعرف على جرائم المعلومات من حيث تعريفها وخصائصها وتقسيماتها ، والجوانب الموضوعية والإجرائية لجرائم المعلومات.

الهدف من الدراسة :

تهدف هذه الدراسة إلى التعرف على التطورات العالمية المعاصرة ، وماهية وحالات وأشكال جرائم المعلومات ، ومن ثم إمكانية تحديد المخاطر المحتملة من جراء انتشار هذه الجرائم.

منهجية الدراسة :

في سبيل تحقيق الهدف من هذه الورقة نسعى لاستخدام منهج التحليل الوصفي ، الذي يركز على استعراض مظاهر الحماية الجنائية الموضوعية والإجرائية المتعلقة بجرائم المعلومات ، إضافة إلى تجميع وتحليل البيانات والمعلومات من المصادر المنشورة المتعلقة بجرائم المعلومات.

تعريف جرائم المعلومات :

نشير بداية أن الفقه انخرط في جدال فقهي في تحديد المقصود بالجريمة ، وحتى يمكن لنا وضع تعريف محدد لتلك الجرائم يتعين أولا أن نلقي الضوء بإيجاز على ذلك الجدل الفقهي ، وثانياً بيان الاصطلاحات المستخدمة للدلالة على تلك الظاهرة :

1- الجدل الفقهي في تحديد المقصود بجرائم المعلومات :

يعتنق جانب من الفقه المعنى الفني لجرائم المعلومات ، حيث عرفها البعض بأنها " نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة ، أو غير مباشرة كوسيلة ، أو هدف لتنفيذ الفعل الإجرامي المقصود " (1).

---

[1]- د. محمد الأمين البشرى ، بحث بعنوان " التحقيق في جرائم الحاسب الآلي " مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت ، المنعقد في الفترة من أول حتى 3 مايو 2000 ، كلية الشريعة والقانون بدولة الإمارات ص

ووفقاً لذلك التعريف يعد الحاسب الآلي هو العنصر المفترض في الجريمة ، لذا يتعين وجود ذلك الحاسب ككيان مادي ملموس ، فضلاً عن أنه يجب أن تتوافر له العناصر المادية ، والمعنوية اللازمة لقيامه ، ويقصد بالعناصر المادية للحاسب الآلي " جميع الأجزاء التي يتكون منها الحاسب الآلي مثل لوحة مفاتيح ، الشاشة الخارجية ، مفتاح التشغيل أي صلاحية جهاز الحاسب الآلي لقبول ومعالجة وتخزين واسترجاع البيانات ".

أما العناصر المعنوية فتشمل المحتوى المعنوي للحاسب الآلي كالبيانات " وهي تعني المعلومات التي يتم تخزينها على جهاز الحاسب الآلي لأجل الانتفاع بها ، واستخدامها أو توثيقها الممتلكات ، وهي تعني دفعات إلكترونية ومعلومات خاصة ، وحقوق نشر محفوظة أو مسجلة بيانات معالجة إلكترونياً ، شفرات تعريف خاصة أو أرقام تسمح بالدخول على الحاسب الآلي ، البرامج القابلة للقراءة ". وعلى ذلك تنقسم الجريمة المعلوماتية من جهة النظر الفنية إلى جرائم العبث بالحاسب الآلي ، الإخلال بأمن الحاسب الآلي ، جريمة غش الحاسب الآلي.

وعلى خلاف من ذلك يرى أنصار الجانب الموضوعي أن " جهاز الحاسب الآلي لا يعد أداة رئيسية في تنفيذ الجريمة ، وإنما تقع الجريمة على الحاسب الآلي ذاته ، أو تقع بداخله " [(1)]. وبالتالي فالجريمة المعلوماتية هي " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب " [(2)].

---

[1]– د/ هشام محمد فريد رستم ، الجرائم المعلوماتية – أصول التحقيق الجنائي الفني واقتـــراح بإنشـــاء آليـــة عربية موحدة للتدريب التخصصي ، بحث مقدم إلى مؤتمر (القانون والكمبيوتر والإنترنت – المنعقد فـــي الفترة من 1–3 مايو 2000) ، كلية الشريعة والقانون بدولة الإمارات ، ص 8.

[2]- Michael Alexander , computer crime , UGLY ,secret for business computer world vol. XXIV,NO.11.1990pp1,4p.104

2- الاصطلاحات المستخدمة للدلالة على جرائم المعلومات :

اختلفت أيضاً الاصطلاحات والمسميات المستخدمة للدلالة على تلك الجريمة ، حيث توصف بجرائم الحاسب الآلي ، جرائم الإنترنت ، جرائم تقنية المعلومات ، جرائم الهاكرز (cyber crime) [1].

أ- جرائم الحاسب الآلي :

هناك جرائم ترتكب بقصد التعدي على المحتوى المادي ، وآخر بقصد التعدي على المحتوى المعنوي.

ب- جرائم التعدي على المحتوى المادي للحاسب الآلي :

وتشمل هذه الجريمة إتلاف أجزاء الحاسب الآلي كلوحة المفاتيح ، وحدة التشغيل أو أي جزء من الأجزاء المادية والتي تدخل في تكوين الحاسب الآلي والعبث به بأي وسيلة ، وقد يصل الأمر إلى حد إتلاف أغلب محتويات الحاسب ، غير أنه يشترط في هذه الحالة بقاء المحتوى المعنوي سليماً ، وهنا تخضع جريمة الإتلاف للتجريم التقليدي المنصوص عليه في قانون العقوبات ما دام المحتوى المعنوي مازال قائماً ويمكن الانتفاع به.

ج- جرائم التعدي على المحتوى المعنوي للحاسب الآلي :

تعد جرائم التعدي على المحتوى المعنوي أكثر الجرائم شيوعاً فيما يتعلق بجرائم المعلومات وعلة ذلك أن هذه الجرائم تنصب على المحتوى المعنوي وتهدف إلى تدمير البيانات والمعلومات أو الدخول غير المشروع على البيانات والمعلومات الخاصة بجهاز الحاسب الآلي بواسطة كلمة المرور (password) ، أو من خلال التعريف الشخصي ، أو المعلومات السرية ، أو سرقة المعلومات [2].

---

[1]- http:www.cybercrime.

[2]- د/ محمد الأمين البشرى ، مرجع سابق ، ص 11 وما بعدها.

د- جرائم الإنترنت :

ومع ازدياد عمليات القرصنة ظهرت جرائم الإنترنت وهي جرائم تختلف عن الجرائم المتعارف عليها ، فالجاني لا يحمل مسدساً ، ولا يسطو على متجر ، فهو جالس في بيته ، ولا يجد عناء في مجرد الضغط على زر يدخل به إلى شبكة الإنترنت ويبدأ في اصطياد ضحاياه ، وجرائم الإنترنت تعددت صورها وأشكالها فلم تعد تقتصر فقط على اقتحام الشبكات وتخـــريبها ، أو سرقة معلومات منها بل شملت أيضاً جرائم أخلاقية مثل الاختطاف ، والابتزاز ، الاحتيال على الأرقام السرية لحسابات عملاء البنوك من خلال اختراق شبكة المعلومات الخاصة بالبنك.

هـ- تعريف جرائم المعلومات :

والمقصود بجرائم المعلومات في رأينا " جميع الأفعال التي ترتكب عمداً ، أو عن طريق الامتناع بالتعدي على جهاز الحاسب الآلي ، أو أي موقع أو نظام إلكتروني ، أو شبكة اتصالات ، سواء كان ذلك النظام شبكة اتصالات دولية ، أو داخلية أو شبكة مصرفية بهدف التعدي على الأموال المادية والمعنوية ، أو إذا وقعت الجريمة بإهمال ، ونشأ عن ذلك التعـــدي على الأموال المادية والمعنوية ، وأفعال التجسس التي تتم عبر الأقمار الصناعية " ومن هذا التعريف الشامل لكافة جرائم المعلومات يتضح الآتي :

- جرائم المعلومات غير واردة على سبيل الحصر :

إذ لا يمكن تحديدها بجريمة واحدة كما دأب الفقه على تسميتها (بالجريمة المعلوماتية) ، لذا فالأدق أن يكون المسمى الدقيق لها (جرائم المعلومات) ، أو (جرائم المعلوماتية) ، وعلة ذلك أنها لا تقع تحت حصر.

- جرائم المعلومات تقع بفعل إيجابي وبطريق الامتناع :

في الأغلب الأعم ترتكب جرائم المعلومات بفعل غير مشروع ينصب على الحاسب الآلي أو المستخدم ، ولا يمكن تحديده مسبقاً نتيجة التطور الهائل في تكنولوجيا المعلومات ،

ومن ثم فهي من الجرائم ذات القالب الحر ، وقد تقع بصورة إيجابية كما هو الأحوال التي يتم فيها اقتحـــام نظام الكمبيوتر للحصول على معلومات ، أو سرقة الرقم السري للفيزا كارت ، أو سرقة المعلومات والأفكار ، أو من خلال القرصنة على الجهاز لنشر فيروسات من خلال (إرسال برامج كمبيوتر بواسطة شبكة الإنترنت ، أو أقراص اليو اس بي (USB) والأقراص المدمجة ، هذه الفيروسات تكرر نفسها وتحطم أنظمة الكمبيوتر ، وتدمر كميات كبيرة من البيانات الهامة [1].

ومن ناحية أخرى تقع عن طريق الامتناع كأن يسمح موظف في أحد الأماكن الحكومية ، أو المؤسسات المالية ، أو مكاتب المحامين بدخول هاكر ، أو قراصنة على الجهاز للحصول على بعض المعلومات الخاصة بأسرار العملاء ، أو الأرقام السرية لبطاقات الائتمان.

- جرائم الحاسب الآلي تشمل التعدي على المحتوى المعنوي :

تشمل جرائم الحاسب الآلي بصفة أساسية التعدي على المحتوى المعنوي ، والذي ينصب على المعلومات ، والأموال والأفكار ، وبالتالي يخرج من نطاق التجريم جرائم التعدي على المحتوى المادي فهي تخضع كما بينا سلفاً لنصوص قانون العقوبات.

- جرائم المعلومات تقع عن طريق الخطأ :

حيث يتصور وقوعها عن طريق الإهمال ، وعلة ذلك في رأينا إمكانية تصور إهمال الجاني في الحفاظ على الأرقام السرية ، أو المعلومات الخاصة بالجهة التي يعمل بها ، مثال إهمال موظف البنك في الحفاظ على سرية أرقام بطاقات الفيزا كارت مما يترتب عليه معرفة هذه الأرقام واستغلالها في سرقة أموال العملاء ، ومن ثم تتحقق الجريمة في صورتها غير العمدية.

---

[1]- http:www.cyberbullying.org-1.

- إمكانية تصور الشروع في جرائم المعلومات العمدية :

الشروع هو البدء في تنفيذ فعل بقصد ارتكاب جناية أو جنحة إذا أوقف أو خاب أثرها لأسباب لا دخل لإرادة الجاني بها ، وبتطبيق ذلك على جرائم المعلومات نرى إمكانية تصور الشروع في هذه الجرائم وبالأخص ما يتعلق منها بجرائم الإنترنت كالشروع في استخدام بطاقة الائتمان المسروقة بسحب أموال المجني عليه من ماكينة الصرف الآلي ، أو الشروع في الدخول عمداً على الحاسب الآلي بقصد إتلاف معلومات أو برامج الحاسب الآلي أو سرقة المعلومات.

- جريمة غش الحاسب الآلي :

تتحقق تلك الجريمة في الحالات التي يدخل فيها مرتكب الجريمة إلى جهاز الحاسب الآلي بحيلة أو خداع أو غش بقصد الحصول على أموال أو ممتلكات [1].

- جرائم التجسس عبر الأقمار الصناعية :

التجسس عبر الأقمار الاصطناعية عملية تسمى (ECHELON) ، وهذه العملية تعتبر تجاوزاً وتعدياً على السيادة الوطنية ، والحريات الشخصية ، بموجبها يجري تسجيل جميع الاتصالات ، في أي مجال (مدني أو عسكري ، اقتصادي أو دبلوماسي) ، ومراقبة حجم الأرصدة في البنوك العالمية ، والتحويلات المالية التي تتم عبر الهاتف المحمول والمتصل عبر القمر الصناعي ، التصنت على المكالمات ، تحديد مكان إقامة بعض الأشخاص المستهدفين بالقتل ، تحديد المواقع عبر أنظمة الأقمار الصناعية بواسطة الكاميرا المدمجة الحديثة والتقاط صور بشكل تلقائي وتعني هذه الخاصية أن الصور التي تم التقاطها لن تحتوي فحسب على تاريخ التقاطها بل أيضاً مكان التقاطها [2].

---

[1]-ILLinois complied statute chapter 120, criminal code , article 16 d, computer crime 1989.

[2]-www.surveillanceissues.com.

و- أهمية دراسة جرائم المعلومات في المجتمع الإلكتروني :

شاع خلال عام 2009 انتشار العديد من جرائم المعلومات ، وبالأخص الاحتيال الإلكتروني ، وسبب ذلك يرجع لانتشار الفيروسات المختلفة ، والبرامج الإباحية ، كما زادت رسائل التهديد الإلكترونية ، وقد شاع مصطلح الهاكرز مقترناً بجرائم المعلومات الجديدة الذي أثار خوف ورعب الكثيرين من مستخدمي الإنترنت من الأفراد ، أو المؤسسات ، الحكومات ، والمنظمات والدول ، بحيث أصبح مؤخراً يشكل أمراً خطيراً.

وقد احتل موضوع الاحتيال التجاري على الإنترنت أهمية كبيرة خلال الآونة الأخيرة نظراً لانتشار استخدامات الإنترنت في كافة مجالات الحياة ، وقد أصدر مركز الشكاوى في الولايات المتحدة في عام 2009 تقريره السنوي الأخير الذي أفاد أن عدد الشكاوى من 1 يناير 2008 – 31 ديسمبر 2008 ، كما تلقى المركز عدد 275284 من الشكاوى أي بما يزيد 33.1% بالمقارنة مع عام 2007 التي قدرت 206884.

وتتعلق أغلب الشكاوى أساساً بجرائم الاحتيال عبر شبكة الإنترنت ، والتزوير الإلكتروني ، وتزوير بطاقات الائتمان والسحب الآلي ، التسلل إلى أجهزة الكمبيوتر ، الرسائل غير المرغوب فيها والإباحية وقد بلغت حجم جرائم الاحتيال 264600000$ أي بواقع خسارة 931.00$ لكل شكوى أي ما يقدر بمبلغ 239100000$ من حجم الخسائر التي أعلن عنها في 2007.

وبعد التحليل السابق لأهمية هذه الدراسة لحجم ما تسببه جرائم المعلومات من أضرار اقتصادية وكذلك بعد استعراض ما أثير من جدل بشأن تعريف جرائم المعلومات والاصطلاحات المستخدمة للدلالة عليها ، انتهينا إلى نقطة هامة وهي " تجريم كافة أنماط السلوك الإجرامي العمدي أو غير العمدي ، وكافة الأشكال المستخدمة في تقنية المعلومات ، يستوي أن تقع الجريمة بواسطة أو على جهاز الحاسب الآلي أو باستغلال شبكة الاتصال

إنترنت أو من خلال التعدي على هذه الشبكة أو إتلافها أو قطع الاتصال بها ، أو من خلال التعدي على حقوق البث الإعلامي عبر الأقمار الصناعية أو انتهاك حقوق الدول والأفراد والشركات من خلال التجسس عبر هذه الأقمار ".

خصائص جرائم المعلومات :

بعد أن بينا تعريف جرائم المعلومات ، نجد أن جرائم المعلومات تتميز وتتصف بمجموعة خصائص هامة :

- سهولة ارتكاب الجريمة لأنها تعتمد على تقنيات ، وآليات مستحدثة ، وتتوقف على مهارات خاصة للجاني قد لا تتوافر في غيره.
- سهولة إخفاء معالم الجريمة لأنها تتم عبر شبكات اتصال ، ومن ثم فهي لا تترك آثاراً مادية وإنما معلومات على جهاز المستخدم يمكن شطبها فور تنفيذ الجاني جريمته.
- سرعة ارتكاب الجريمة لاعتمادها على وسائل الاتصال الحديثة.
- تتصف الجريمة بالصعوبة في الإثبات ، لأن دليل الإثبات ليس من الأدلة التقليدية التي نصت عليها القوانين الإجرائية ، وإنما دليل فني يحتاج إلى تقنيات فنية وأجهزة متخصصة للكشف عن محتواه.
- جرائم المعلومات ليست من الجرائم المادية وإنما تصيب المحتوى المعنوي أي البيانات والبرامج والمعلومات والأفكار والممتلكات والأموال.
- الأغلب الأعم من هذه الجرائم يتسم بالطابع الدولي فهي تتم عبر الحدود مما يؤدي إلى صعوبة التوصل إلى الجاني ، وعدم فاعلية الإجراءات التي تتخذ ضده.
- خطورة هذه الجرائم أنها ترتكب بواسطة أصحاب الياقات البيضاء من خلال الاحتيال على البنوك ، بل تطورت الجريمة إلى حد أنها أصبحت تسهل عمليات غسل الأموال المتحصلة من مصادر غير مشروعة ، وذلك من خلال استخدام التحويلات الإلكترونية لإضفاء المشروعية على الأموال غير المشروعة.

- وأخيراً باتت جرائم المعلومات تستخدم في جرائم الإرهاب من خلال تهديد الأشخاص عبر المواقع بارتكاب أنشطة إرهابية ، بل أن أعمال القرصنة أصبحت تستخدم على نطاق المواقع العسكرية ، وهو ما يسمى بالحرب عبر الإنترنت.

تصنيف أشكال جرائم المعلومات :

على الرغم من وجود العديد من التصنيفات لأشكال جرائم المعلومات ، إلا أن هذه الدراسة تركز على أهم جرائم المعلومات وأكثرها شيوعاً وذلك كما يلي :

أولاً – تصنيف الجرائم حسب مساسها بالأموال :

1- **جرائم الاحتيال على البنوك** : لا تقتصر جرائم المعلومات على الإخلال والعبث بأمن الحاسب الآلي بالدخول غير المشروع على برامج ومعلومات الحاسب الآلي ، بل تستطيل لتشمل الجرائم التي تتم عبر شبكة الإنترنت ، وأبرزها جرائم الاحتيال على البنوك ، والتي تتم عن طريق اختراق النظام المعلوماتي للبنك ، ومعرفة أرقام حسابات العملاء ، وسحب هذه الأموال من حسابهم عن طريق الهاكر ، وتسمى جرائم ذوي الياقات البيضاء white-collar crime [(1)].

2- **جرائم الاحتيال التجاري على الأشخاص** : يقع الاحتيال على الأشخاص عبر الإنترنت من خلال الشات ، أو رسائل على البريد الإلكتروني ، مثال إعلان تاجر عن بيع سيارات رخيصة الثمن بالمزاد عن طريق الإنترنت ، فيقوم المتسوق الإلكتروني بالشراء ، وتحويل الأموال للتاجر ثم يتبين بعد ذلك احتيال التاجر ، وأن الصفقة وهمية.

ومن ناحية أخرى قد يحدث الاحتيال من جانب المشتري باستخدام بطاقة ائتمان وهمية لا وجود لها بتوجيه رسالة إلى التاجر على البريد الإلكتروني الخاص به

[1]-Federal Bureau of Investigation Retrieved 2010-08 http://www.fas.org/irp/agency/doj/fbi/2009just.pdf "Congressional budget justification, FY 2009" and Research Centers White Collar Crime, simultaneously in Canada, United States of AmericaCopyright @ D.C. Heath and Company-1982p 5.

تتضمن الرغبة في شراء بعض البضائع ولكن على متن سفينة ، وأن لديه بطاقات الائتمان وعند العودة سيقوم بتحويل الأموال له ، ويزيل رسالته بعنوان وبريد إلكتروني وهمي وبمجرد وصول البضاعة إليه يتبين عدم وجود بطاقة ائتمان ، وبالتالي لا يحصل التاجر على مقابل البضاعة ، وقد يرتكب الجاني الاحتيال عبر شبكة الإنترنت باستغلال حاجة بعض الأشخاص للوظائف وإيهامهم بالحصول على وظيفة كمندوب لشركة تجارية كبرى ، ويطلب منهم دفع الضريبة عن الشركة مقابل الحصول على عمولة ، لأن القانون يلزم الشركات بدفع ضريبة 25% ، في حين أن الفرد العادي يدفع 7% فقط وأن الشركة ستبرم الصفقات باسمه وبمجرد تحويل المبلغ المزعوم إلى الشركة يكتشف الشخص أنها شركة وهمية ولا وجود لها ، وكذلك قد يحتال شخص على آخر بإيهامه بأنه فاز في اليانصيب بمبلغ كبير يصل إلى ملايين من الدولارات وأنه يحتاج لمبلغ من المال كضريبة للإفراج عن ذلك المبلغ [1].

ثانياً- تصنيف الجرائم حسب خطورتها :

1- الإرهاب الحاسوبي (cyber terrorist) : وضع هذا المصطلح من قبل الفقيه الأمريكي " كولين باري جيم " ، وقد عرف معهد تكنوليتيكسفي واشنطن الإرهاب الحاسوبي " أنه التخريب والتهديد التي ترتكب عمداً عبر شبكات الاتصال ، بهدف التسبب في اضطرابات اجتماعية ، أو دينية أو سياسية ، أو ما شابه ذلك من أهداف أيديولوجية ، أو لتخويف أي شخص وذلك تعزيزاً لهذه الأهداف " [2] ، وفي ذات السياق عرف المؤتمر الوطني للمجالس التشريعية في واشنطن (National

[1]-Jamie Doward (2008-03-09 .("How boom in rogue ticket websites fleeces Britons" . TheObserverLondon . http://www.guardian.co.uk/world/2008/mar/09/olympicgames2008.internet . Retrieved 9 March 2008.

[2]-Anderson, Kent (October 13, 2010). "Virtual Hostage: Cyber terrorism and politically motivated computer crime". The Prague Post. http://praguepost.com/opinion/5996-virtual-hostage.html. Retrieved 2010-10-14.

(Conference of State Legislatures الإرهاب الحاسوبي بأنه " استخدام تكنولوجيا المعلومات من قبل الجماعات الإرهابية ، بإطــلاق التهديدات Denial-of –service attack لتنظيم وتنفيذ هجمات إرهابية ، أو لتبادل المعلومات بشأن قضايا الإرهاب إلكترونياً كالتهديدات الإرهابية عبر وسائل الاتصال الإلكترونية بإحداث تفجيرات إذا لم تستجب الدولة لمتطلبات سياسية " [1].

2- **حرب الإنترنت (Cyber War)** : برز في الآونة الأخيرة ما يسمى بحرب الإنترنت وهو استخدام شبكة الإنترنت في القرصنة على الدول من أجل تحقيق أهداف عسكــرية ، ففي عام 2007 تم الهجوم على نظام المعلومات العسكري لدولة أستونيا ، على أيدي قراصنة روس ، وفي أغسطس 2008 أجرت روسيا مرة أخرى عمليات قرصنة على الكمبيوتر على جورجيا ، وقد بات من الممكن في المستقبل أن تحل حرب الإنترنت بين الدول بدلاً من القتال المسلح [2]. وفي مارس 2010 ضبط المحققون الأسبان فيروسات على أجهزة الكمبيوتر ترتب عليها خسارة ثروات طائلة لحوالي 1000 شركة وأكثر من 40 بنكاً [3].

ثالثاً- تصنيف الجرائم حسب استغلال جهاز الحاسب الآلي كأداة للجريمة :

1- **التزوير في التوقيع الإلكتروني** : تقع جريمة التزوير في التوقيع الإلكتروني باستخدام الماسح الضوئي (Scanner) بنقل التوقيع الخطي كما هو إلى وثيقة محفوظة على جهاز الحاسب الآلي لكي يتم مهرها بهذا التوقيع ، وبذلك تكون الرسالة ، أو المستند موقعة من صاحب الشأن ، أو باختراق الجاني جهاز الحاسب

1-What is cyberterrorism? Even experts can't agree. Harvard Law Record. VictoriaBaranetsky. November 5, 2009.- http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA439217.

2-"War is War? The utility of cyberspace operations in the contemporary operational environment" U.S. Army War College, February 2010.

3- Mann, D. and Sutton, M. (1998) >>Netcrime: More Change in the Organization of Thieving. British Journal of Criminology. 38:PP. 201-229 Oxfordjournals.org.

الآلي ، والتوصل إلى الرسالة أو المستند الموقع ثم يحتفظ لنفسه بنسخة من التوقيع ويقــوم هو بدوره بنقله إلى أي مستند آخر لاصطناع سند مديونية ، أو التزام قانوني ، ومما لا شك فيه أن هذا النوع من أنواع التوقيع لا يتمتع بأي درجة من درجات الأمان التي يمكن أن تحقق الثقة اللازمة في التوقيع ، إذ أن المرسل إليه يستطيع أن يحتفظ بنسخة من صورة التوقيع ويعيد لصقها على أي وثيقة من الوثائق المحررة على الوسائط الإلكترونية ، لذلك فإن هذا النوع من التوقيع الإلكتروني لا يمكن للقضاء الاعتداد به في استكمال عناصر الدليل الكتابي المعد للإثبات [(1)]. إلا إذا كان ذلك التوقيع محمياً بموجب نظام قانوني/ وأن يكون هناك سجل إلكتروني/ وكانت الرسالة ، أو التوقيع الإلكتروني أفضل دليل يمكن أن يحصل عليه الشخص الذي يستشهد ما لم يثبت العكس " [(2)].

2- **تزوير بطاقات الائتمان** : هو مصطلح واسع النطاق يشمل السرقة والتزوير التي ترتكب على بطاقات الائتمان ، أو أي آلية دفع مماثلة ، حيث يتم سرقتها من مالكها الأصلي واستغلالها في الحصول على بضائع دون دفع مقابل ، أو الحصول على أموال من الحساب identity theft ، ثم التوقيع على فاتورة الشراء بتوقيع مزور ينسبه إلى المالك الأصلي للبطاقة [(3)].

وغالباً ما يستخدم الجاني بطاقات الائتمان المسروقة في الخدمة الذاتية أنظمة الدفع (محطات البنزين ، أماكن التسوق وغيرها) هي أماكن تعد أهداف مشتركة للبطاقات المسروقة ، ولا سيما وأنه لا توجد وسيلة للتحقق من هوية حامل البطاقة ، وحتى يمكن التغلب على ذلك في رأينا يتعين أن يطلب من المستخدم إجراء المعاملة إدخال

---

[1]- د. حسن عبدالباسط جميعي ، إثبات التصرفات القانونية التي تم إبرامهـا عــن طريــق الإنترنــت ، دار النهضة العربية ، مصر 2000م ، الطبعة الأولى ، ص 35.

[2]- حكم محكمة التمييز ، دبي بتاريخ 2008/1/28 في الطعن رقم 2007/ 241 طعن تجاري.

[3]-"Consumer Sentinal Network Data Book: January - December 2008" (PDF). Federal Trade Commission. February 26, 2009. http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf. Retrieved 2010-02-21

بعض المعلومات التعريفية ، مثل الرمز البريدي للمستخدم ، بيانات رخصة القيادة ، العنوان ، تاريخ الميلاد ، وقد يتم تزوير بطاقة الائتمان باستخدام جهاز صغير الإلكتــروني يقوم بتخــزين وتسجيل أرقام بطاقات الائتمان Security Card Code [1].

3- **التزوير في البطاقات البلاستيكية** : يتحقق التزوير في البطاقة البلاستيكية عن طريق نسخ كافة بيانات البطاقة بواسطة وضع شريط تسجيل إلكتروني على البطاقة الأصلية ثم تمرير تيار حراري له خاصية ، حيث تحصل عملية نسخ البيانات من البطاقة الأصلية إلى الشريط الممغنط ثم بعد ذلك تأتي عملية التزوير حيث يوضع الشريط الممغنط الذي تم نسخ المعلومات عليه على الشريط الممغنط الفارغ ومن ثم العمل بنفس خطوات العملية الأولى وذلك بتمرير ذات التيار حيث تنسخ البيانات إلى الشريط الفارغ ، وتسمى هذه العملية بالإدخال ، وهي في عملها تشبه مبدأ عمل الماسح الضوئي (Scanner) ، كما يمكن أيضاً تركيب جهاز النسخ على فتحة إدخال البطاقة ، بحيث تتم عملية نسخ المعلومات عند إدخال البطاقة حيث تمرر البطاقة أيضاً في جهاز النسخ ، ويحصل الجاني على بيانات ومعلومات لبطاقة صحيحة ، وقد كشف البنك المركزي الإماراتي عن تمكن عصابة من خبراء في علوم الحاسب الآلي من استخدام هذه الآلية في الإمارات العربية المتحدة ، حيث تعرضت مصارف متعددة لتزوير بطاقات الائتمان [2].

4- **سرقة بيانات بطاقات الائتمان** : سرقة البيانات أو المعلومات الخاصة بأرقام بطاقات ويتحقق ذلك من خلال شبكة الإنترنت ، واستغلال هذه المعلومات في سرقة أموال العملاء عن طريق شبكة الإنترنت المصرفية أو بيع هذه المعلومات للآخرين.

1- "Credit Card Issuer Fraud Management, Report Highlights, December, 2008". Mercator Advisory Group. 2008.
http://www.sas.com/news/analysts/mercator_fraud_1208.pdf

2- محمد حماد مهرج الهيتي ، الحماية الجنائية لبطاقات الائتمان الممغنطة ، دار الكتب القانونية ، دار شتات للنشر والبرمجيات ، ص 46 ص 256.

5- **غسل الأموال عن طريق تكنولوجيا المعلومات :** يعد التحويل عن طريق شبكة الإنترنت من أبرز التحويلات التي تتم في العصر الحديث ، لذا قد يستغل غاسلو الأموال التحويلات الإلكترونية لتحويل الأموال المتحصلة من جرائم إلى أموال مشروعة ، ويرجع ذلك إلى سهولة نقلها عبر الشبكة من عميل إلى آخر ، وتشير الإحصاءات أن حجم الأموال غير المشروعة التي تقوم المؤسسات المالية بتحويلها إلكترونياً تقدر بمبلغ بليون $ يومياً [1].

وعلى ذلك تبنت منظمة FATF توصيات خاصة بمكافحة غسل الأموال وتمويل الإرهاب في التوصية السابعة الصـــادرة سنة 2005 بفرض رقابة على التحويلات الإلكترونية ، بحيث يجب على الدول أن تتخذ تدابير لإلزام المؤسسات المالية عند تحويل الأموال ، الحصول على معلومات دقيقة ، مثل الاسم ، والعنوان ورقم الحساب الخاص بعمليات تحويل الأموال والرسائل المرسلة ، كما ينبغي أن تظل المعلومات الخاصة بنقل الرسالة لإجراء فحص دقيق ، ورصد للأنشطة المشبوهة لتحويل الأموال [2].

ونجد أن المشرع الأمريكي يشدد عقوبة جريمة غسل الأموال المتحصل من جرائم الاحتيال على المؤسسات المالية في القسم 1956 من قانون السيطرة على أفعال غسل الأموال الصادر سنة 1982 إلى السجن مدة لا تجاوز ثلاثين سنة أو بغرامة لا تزيد على مليون $ أو العقوبتين معاً عند ارتكاب الجاني أو الشروع أو التخطيط في ارتكاب جريمة النصب على المؤسسات المالية ، لسلب أموالها بأي وسيلة ، عن طريق الاحتيال الإلكتروني على الموظفين في البنوك لسلب أموال المودعين ، وغالباً ما تتحقق هذه الجريمة

1- د. محمود شريف بسيوني ، غسل الأموال والاستجابة الدولية وجهود المكافحة الإقليمية والوطنيـــة ، دار الشروق – طبعة 2004 ، ص 65-74.

2- Financial Action Task Force on Money Laundering , & Terrorist financing : typologies reports 2005 FATF-IXhttp://www.fatf-gafi.org/pdf/TY1998_en.pdf.

باستغلال الجاني للتقنيات الحديثة ، كالدخول على شبكة الإنترنت ومعرفة الرقم السري لبطاقات العملاء ، وسحب أموالهم المودعة بالبنوك " [1].

لقد اتضح من تعريف جرائم المعلومات وخصائصها مدى تعدد واختلاف جرائم المعلومات بشكل قد يصعب معه حصرها ، الأمر الذي يعكس مدى تنامي التطور الهائل في تكنولوجيا المعلومات والاتصالات ، ومع ذلك تبقى حقيقة هامة " أن هذه الجرائم إما أن تقع على المعلومات ، والبيانات الخاصة بأجهزة الحاسب الآلي ، أو على شبكة الاتصال (إنترنت) ، أو تزوير وسرقة بطاقات الائتمان أو المستندات الإلكترونية ، أو غسل الأموال غير المشروعة عن طريق الإنترنت ، أو التجسس بواسطة الأقمار الصناعية ، أو على الحقوق الناشئة عنها ، ومن ثم بات جهاز الحاسب الآلي وشبكة الإنترنت والأقمار الصناعية عناصر رئيسية في جرائم المعلومات ". إلا أنه لا يزال هناك كثير من الجدل الفقهي والتشريعي حول العديد من التساؤلات عن الأشكال الفعلية لجرائم المعلومات ويمكن تحديد أهم تلك التساؤلات فيما يلي : هل تتوافر الحماية الجنائية الموضوعية والإجرائية اللازمة ضد جرائم المعلومات ؟ للإجابة عن تلك التساؤلات من الضروري بيان مظاهر الحماية الجنائية الموضوعية والإجرائية ضد جرائم المعلومات ، وذلك ما تسعى إليه هذه الدراسة في النقطة التالية.

الحماية الجنائية الموضوعية والإجرائية ضد جرائم المعلومات :

يقصد بالحماية الجنائية الموضوعية النصوص القانونية التي تتناول بالتجريم والعقاب جرائم المعلومات ، ومدى كفايتها لبسط الحماية الكافية ضد هذه الجرائم ، ويقصد بالحماية القواعد الإجرائية المتعلقة بالجهة المختصة بالاستدلال والقبض والتفتيش ، والدليل المعلوماتي ومقوماته.

[1] – انظر مؤلفنا في جريمة غسل الأموال دراسة مقارنة ، منشأة المعارف ، طبعة 2008 ، ص 272.

1- الحماية الجنائية الموضوعية ضد جرائم المعلومات :

لما كان تركيز هذه الدراسة على جرائم المعلومات بقصد الوصول إلى أنسب الحلول لمكافحتها ، فإنه من الواجب الاقتصار على بعض النماذج التشريعية ، لذا سنختار من بين هذه النماذج القانون الإماراتي والقانون الفرنسي باعتبارهما من التجارب التشريعية الحديثة.

أولاً – قانون العقوبات الاتحادي :

تضمن قانون العقوبات الاتحادي رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات الجرائم الآتية :

- الدخول عمداً بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به.
- تزوير مستند من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية معترف به قانوناً في نظام معلوماتي ، أو غير ذلك من مستندات.
- إعاقة أو تعطيل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بأية وسيلة كانت عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.
- الدخول عمداً عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات ، ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات فيها يعاقب بالسجن المؤقت وبالغرامة التي لا تقل عن خمسين ألف درهم أو بإحدى هاتين العقوبتين.
- تعديل أو إتلاف الفحوصات الطبية ، أو التشخيص الطبي ، أو العلاج الطبي ، أو الرعاية الطبية ، أو التهسيل للغير فعل ذلك ، أو التمكين منه ، باستعمال الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.
- كل من تنصت أو التقط أو اعترض عمداً دون وجه حق ، ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات ، يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين.

- كل من استعمل الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في تهديد أو ابتزاز شخص آخر لحمله على القيام بفعل أو الامتناع عنه.
- كل من توصل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند ، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه.
- كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول دون وجه حق إلى أرقام أو بيانات بطاقة ائتمانية أو غيرها من البطاقات الإلكترونية.
- كل من أنتج أو أعد أو هيأ أو أرسل أو خزن بقصد الاستغلال أو التوزيع أو العرض على الغير عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات ما من شأنه المساس بالآداب العامة أو أدار مكاناً لذلك.
- كل من حرض ذكراً أو أنثى على الدعارة أو الفجور أو ساعده على ذلك باستخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.
- كل من دخل بدون وجه حق ، موقعاً في الشبكة المعلوماتية لتغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه.
- كل من ارتكب إحدى الجرائم التالية عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات – الإساءة إلى أحد المقدسات أو الشعائر الإسلامية – الإساءة إلى أحد المقدسات أو الشعائر المقررة في الأديان الأخرى متى كانت هذه المقدسات والشعائر مصونة وفقاً لأحكام الشريعة الإسلامية – سب أحد الأديان السماوية المعترف بها – حسن المعاصي أو حض عليها أو روج لها.
- كل من اعتدى على أي من المبادئ أو القيم الأسرية أو نشر أخباراً أو صوراً تتصل بحرمة الحياة الخاصة أو العائلية للأفراد ، ولو كانت صحيحة ، عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.
- كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات ، بقصد الاتجار في الأشخاص أو تسهيل التعامل فيه.

- كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات ، بقصد ترويج المخدرات أو المؤثرات العقلية وما في حكمها أو تسهيل التعامل فيها وذلك في غير الأحوال المصرح بها قانوناً.
- كل من قام باستخدام أو اكتساب أو حيازة الأموال مع العلم بأنها مستمدة من مصدر غير المشروع أو بتحويل الموارد أو الممتلكات مع العلم بمصدرها غير المشروع ، وذلك عن طريق استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد إضفاء الصفة المشروعة على تلك الأموال أو أنشأ أو نشر معلومات أو موقعاً لارتكاب أي من هذه الأفعال.
- كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لأية مجموعة تدعو لتسهيل وترويج برامج وأفكار من شأنها الإخلال بالنظام العام والآداب العامة.
- كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى سوائل تقنية المعلومات لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها ، أو أعضائها ، أو ترويج أفكارها ، أو تمويلها ، أو نشر كيفية تصنيع الأجهزة الحارقة ، أو المتفجرة ، أو أية أدوات تستخدم في الأعمال الإرهابية.
- كل من دخل وبغير وجه حق موقعاً أو نظاماً مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك ، أو إذا دخل على تلك البيانات وقام بإلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها.
- ويعاقب أيضاً كل من حرض أو ساعد أو اتفق مع الغير على ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون ووقعت الجريمة بناء على هذا التحريض ، أو المساعدة ، أو الاتفاق يعاقب بذات العقوبة المقررة لها.

وفي ضوء العرض المتقدم ، يمكن الوقوف على أن المشرع الإماراتي اعتمد في التجريم على الطابع العمدي ، حيث يلزم توافر القصد الجنائي ، وبالتالي يخرج من نطاق التجريم الأفعال غير العمدية ، كما اعتمد في تصنيف الجرائم على أربع نقاط رئيسية **أولها** تجريم جميع الأفعال التي تنطوي على الإخلال والعبث بأمن الحاسب الآلي كحذف وتدمير البيانات ، **ثانيها** تجريم الأفعال التي تتعلق بجرائم الإنترنت كإعاقة أو تعطيل الوصول إلى الخدمة ، أو إيقاف العمل بها ، تعديل أو إتلاف أي مستندات طبية ، أو التسهيل للغير فعل ذلك ، **ثالثها** تجريم جميع الأفعال التي ترتكب عن طريق وسائل تقنية المعلومات يستوي في ذلك الاستيلاء على الأموال ، أو الوصول بدون وجه حق إلى أرقام وبيانات البطاقة الائتمانية أو جرائم التحريض على الدعارة ، أو الإساءة إلى المقدسات الدينية ، **وأخيراً** تزوير التوقيع والمستندات الإلكترونية.

ثانياً – قانون العقوبات الفرنسي :

تناول القانون الفرنسي بالتجريم جرائم الإخلال بأمن الحاسب الآلي ومكوناته ، وجرائم الإنترنت حيث تنص المادة 4/335 من القانون رقم 763 لسنة 2006 بشأن مكافحة جرائم المعلومات على أنه يعاقب بالغرامة " كل من استخدم جهازاً أو تكنولوجيا أو أي شيء أعد خصيصاً لإزالة أو تغيير أي معلومات أو سرقة حقوق الملكية الفكرية والمعلومات أو حقوق النشر أو أي حقوق متعلقة بقاعدة بيانات ذات صلة أو ممتلكات ، أو أخفاها أو سهل للغير ذلك ، كل من استخدم خدمة مصممة أو مكيفة خصيصاً لنقل البيانات المشار إليها في الفقرة السابقة ويخرج من نطاق التجريم الأفعال التي لا تصيب الغير بأي أضرار أو كانت تتعلق بأغراض بالأمن أو للبحث العلمي في علم التشفير ". كما تنص المادة 5/335 على أنه يعاقب " بالغرامة كل من تسبب بالإهمال الجسيم ، في دخوله على جهاز الحاسب المملوك لأي شخص دون أي سبب وجيه ، أو مكن الغير بإهمال في الحصول على خدمات الاتصالات على الإنترنت ، شرط أن يتوافر لديه الإهمال ولا يتخذ قواعد الحيطة والحذر ويستوي أن يكون المجني عليه قد وضع وسيلة لتأمين الدخول

على الجـــهاز من عدمه " وطبقاً للمادة 335-7-1 " يجوز الحكم على مرتكبي الجريمة بالسجن والحكم بعقوبة تكميلية وهو وقف توصيل خدمات الاتصال عبر الإنترنت لمدة أقصاها شهر واحد " [1].

مما سبق يتضح أن المشرع الفرنسي في جرائم المعلومات جرم أي تقنيات ، أو تكنولوجيا مستخدمة يستخدمها المجرم المعلوماتي في سرقة المعلومات ، أو الأموال عبر شبكة الإنترنت ، علاوة على أنه أقر بعقاب الجاني عن الجريمة في صورتها غير العمدية وهو اتجاه مميز نأمل أن تقتدي به أغلب التشريعات العربية.

1-Article R335-5 En savoir plus surcet article...Créé par Décret n°2010-695 du 25 juin 2010 - art.

-Constitueunenégligencecaractérisée, punie de l'amendeprévue pour les contraventions de la cinquièmeclasse, le fait, sans motif légitime, pour la personnetitulaire d'un accès à des services de communication au public en ligne, lorsque se trouventréunies les conditions prévues au II :

-°Soit de ne pas avoirmis en place un moyen de sécurisation de cetaccès ;

-° Soitd'avoir manqué de diligence dans la mise en œuvre de cemoyen.

II.-Les dispositions du I ne sontapplicablesquelorsque se trouventréunies les deux conditions suivantes :

1°En application de l'article L. 331-25 et dans les formesprévues par cet article, le titulaire de l'accès's'est vu recommander par la commission de protection des droits de mettre en œuvre un moyen de sécurisation de son accèspermettant de prévenir le renouvellementd'uneutilisation de celui-ci à des fins de reproduction, de représentationou de mise à disposition ou de communication au public d'œuvresoud'objets protégés par un droitd'auteurou par un droitvoisin sans l'autorisation des titulaires des droitsprévus aux livresIer et II lorsqu'elleestrequise

-°Dansl'annéesuivant la présentation de cetterecommandation, cetaccèsest à nouveau utilisé aux fins mentionnées au 1° du présent II.

III.-Les personnescoupables de la contravention définie au I peuvent, en outre, êtrecondamnées à la peinecomplémentaire de suspension de l'accès à un service de communication au public en ligne pour uneduréemaximale d'un mois, conformément aux dispositions de l'article L. 335-7-1.

http://www.legifrance.gouv.

2- الحماية الجنائية الإجرائية ضد جرائم المعلومات :

تثير الجرائم المتعلقة بالمعلومات بعض المشاكل والصعوبات في الجهة المختصة بالاستدلال والتحقيق وعلة ذلك أن هذه الجرائم تتعلق بمعلومات وبيانات ، أو شبكة اتصال مما يجعلها تختلف عن الجرائم التقليدية ، وأغلب التشريعات عندما تناولت هذه الجرائم تعرضت لها من حيث الجانب الموضوعي دون الجانب الإجرائي ، ومن ناحية أخرى تثور صعوبات في مرحلة المحاكمة فيما يتعلق بدليل إثبات الجريمة ، ومقوماته ، ولا سيما أنه في محيط جرائم المعلومات لا يستطيع القاضي تطبيق إجراءات الإثبات التقليدية ، وعلة ذلك أن هذه الجرائم ذات طبيعة معنوية [1].

ووفقاً لنصوص المواد 23 ، 24 ، 25 ، 26 من القانون العربي النموذجي تطبق أحكام قانون الإجراءات الجزائية في شأن القانون الواجب التطبيق ، وإجراءات الاستدلال ، والقبض والتفتيش في جرائم المعلومات [2].

أولاً- القانون الواجب التطبيق :

أغلب التشريعات الجزائية تأخذ بمبدأ الإقليمية فيطبق القانون على أي جريمة ترتكب داخل القطر ، ويترتب على ذلك أن الاختصاص ينعقد لمجرد وقوع أحد العناصر المكونة للجريمة ، فقيام شخص في الخارج ببث رسائل تهديدية ، أو صور إباحية لشخص آخر داخل الإقليم يجعل القانون الواجب التطبيق هو قانون ذلك الإقليم [3] ، ورغم أن الرسالة

1- د/ محمد محي الدين عوض ، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة من 25 إلى 28 أكتوبر.

2- المستشار الدكتور/ عبدالفتاح بيومي حجازي ، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت ، دار الكتب القانونية ، 2007 ، ص 69.

3- د/ محمد محي الدين عوض ، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة من 25 إلى 28 أكتوبر.

صدرت من الخارج ، لأن تلقي المستخدم لهذه الرسالة على إقليمه يعد أحد العناصر المكونة للجريمة [1].

وقد أكدت ذلك المادة 113-2 عقوبات فرنسي والتي تنص على أنه " يطبق القانون الفرنسي على الجرائم المرتكبة على إقليم الجمهورية ، وتعتبر الجريمة قد ارتكبت على إقليم الجمهورية إذا كان أحد عناصر الجريمة قد وقع على هذا الإقليم " [2].

ولكن تثور مشكلة بشأن جرائم الإنترنت تتعلق بابتعاد المجرمين عن سلطة الدولة المتضررة من الجريمة وإفلاتهم من العقاب ، وعلة ذلك أن هذه الجرائم عابرة للحدود ، الأمر الذي يقتضي إما أن تقوم الدولة التي يتواجد المتهم بارتكاب إحدى جرائم الإنترنت بمحاكمته ، أو بتسليمه للدولة المتضررة لمحاكمته ، وهو ما يعرف بنظام تسليم المجرمين ، وعلى هذا الأساس لجأت أغلب الدول إلى عقد اتفاقيات ثنائية بشأن تسليم المجرمين ، ويعتد بهذه الاتفاقيات ، وقد أكدت ذلك اتفاقية الجريمة الإلكترونية الصادرة بتاريخ 2004/7/1 من مجلس أوروبا في المادة الحادية عشرة بعنوان مبادئ التسليم [3].

1- د/ جميل عبدالباقي الصغير ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت ، دار النهضة العربية ، طبعة 2002 ، ص 47-48.

2- www.lemondepolitique.fr/cours/droit_penal/general/application_loi_penale.html.

3- تطبـق هذه المادة على التسليم بين الأطراف بالنسبة للجرائم الجنائية المقامة بما يتفق مع من هذه الاتفاقية ، شريطة أن تكون موجبة للعقاب بموجب القوانين السارية في كلا الطرفين المعنيين بالحرمان من الحرية الشخصية لفترة قصوى من عام واحد على الأقل ، أو بعقوبة أكثر تشددا (ب) حيث يتقرر تطبيق عقوبة دنيا مختلفة بموجب ترتيب متفق عليه على أساس من تشريع موحد أو متبادل أو على أساس معاهدة تسليم ، بما في ذلك معاهدة التسليم الأوروبية (ETS No. 24) ، والمطبقة بين طرفين أو أكثر ، تطبق العقوبة الدنيا المنصوص عليها بموجب هذا الترتيب أو هذه المعاهدة.

ثانياً- إجراءات الاستدلال :

إجراءات الاستدلال يختص بها مأمور الضبط القضائي كاختصاص أصيل وفي جرائم المعلومات قامت بعض الدول بإنشاء جهاز ضبط قضائي يناط به إجراءات الاستدلال كجهاز (FBI) في الولايات المتحدة ، وفي مصر (إدارة مكافحة جرائم الحاسب الآلي) ، وفي الإمارات أنشأت شرطة متخصصة ضمن إدارة المباحث والجرائم الإلكترونية.

وأبرز إجراءات الاستدلال هي التحري والبحث وفي الجرائم المعلوماتية ، حيث يجوز البحث والتحري من خلال رصد التحركات التي تتم عبر الإنترنت والرسائل من خلال نظام (PROXY) وهو نظام أمني وتحكم في المواقع يمكن من خلاله مراقبة شبكة الاتصال ومنع الدخول على مواقع معينة كالمواقع التي تعرض أفلاماً مخلة بالآداب ، غير أنه لا يجوز الاطلاع على هذه الرسائل إلا بالحصول على إذن النيابة العامة.

ثالثاً- التفتيش والقبض :

يقصد بالتفتيش في النظام المعلوماتي إجراء تقوم به سلطات التحقيق لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى متهم بارتكابها.

وتخضع إجراءات التفتيش وما يستتبعها من قبض إلى القواعد الواردة في قانون الإجراءات الجزائية بضرورة الحصول على إذن سلطات التحقيق للاطلاع على الرسائل عبر شبكة الإنترنت أو لضبط جهاز الحاسب الآلي وفك شفرته ، والاطلاع على ما يحتويه من معلومات ، وإن كان من الملائم التدخل التشريعي بوضع نصوص تبيح للنيابة العامة حق ندب مأموري الضبط القضائي لمراقبة شبكة الإنترنت ، شرط أن تكون هناك جريمة وقعت بالفعـل وتأرجحت نسبتها إلى مرتكبها ، وأن تكون المراقبة بهدف ضبط أدلة

الجريمة ، وكذلك إعطاؤه الحق في تفتيش جهاز الحاسب الآلي إذا توافرت دلائل كافية على الاتهام بارتكاب جريمة أو بصدور إذن من الجهة المختصة ، بل يتصور في رأينا توافر حالة التلبس في هذه الجرائم عند مشاهدة مأموري الضبط القضائي رسائل إباحية على جهاز أحد الأشخاص عرضاً ، أو تلقيه بلاغاً من أحد مقاهي الإنترنت بقيام أحد الأشخاص بارتكاب جريمة عبر الإنترنت فيتوجه لفحص البلاغ ويشاهد الجاني على سبيل المثال يرتكب جريمة الاحتيال أو التهديد.

رابعاً- الدليل المعلوماتي :

ولما كان تركيز هذه الورقة على جرائم المعلومات ، فإنه من الواجب الاقتصار على أهم الأدلة المعلوماتية ، وهي الحاسب الآلي – المعاينة – تقرير الخبرة.

- **استخدام الحاسب الآلي كدليل إثبات في جرائم المعلومات :** يعد جهاز الحاسب الآلي الأداة الرئيسية في تنفيذ الجريمة ذلك لأن استخدام الجاني لشبكة الإنترنت في بث رسائل تهديد أو بالدخول على موقع إلكتروني لإتلاف برامج وبيانات يتم عن طريق جهاز حاسب آلي يتم توصيله بشبكة اتصال ، لذا يمكن من خلال مراقبة ذلك الجهاز بإذن السلطات ضبط الإشارات التي تصدر من الجهاز الخاص به ، وبذلك يعد جهاز الحاسب دليلاً في إثبات الجريمة ، مثال قضية القرصان " Kevin Mitnick " الذي أتهم بسرقة معلومات أحد الأشخاص عن طريق جهاز حاسب آلي تم توصيله بخط اتصال بتليفون محمول وقد قامت السلطات بوضع جهاز التقاط الإشارات واستطاعت تحديد مكان قراءة المعلومات وتم ضبط المتهم حال استخدامه الجهاز في قراءة المعلومات (1).

1- United States Attorney'sOffice ,Central District of California (9 August 1999). "KevinMitnick sentenced to nearly four years in prison; computer hacker ordered to payrestitution to victim companies whose systems were compromised". Pressrelease .http://www.usdoj.gov/criminal/cybercrime/mitnick.htm.

- **معاينة جهاز الحاسب الآلي** : تعد المعاينة من إجراءات التحقيق ، ولا تملك جهات الاستدلال القيام بها إلا في حالات استثنائية يصعب تصورها في جرائم المعلومات وتقتصر فقط على ما يتعلق بأمن المعلومات فقط ، لذا يتعين في جرائم المعلومات قيام النيابة العامة بتصوير النظام المعلوماتي وما يتصل به من أجهزة ، إثبات حالة التوصيلات والكابلات ، حفظ الأوراق والأقراص ومخرجات الأجهزة المعلوماتية ، ومن ثم يجوز التعويل على هذه المعاينة كدليل في إثبات الجريمة.
- **تقرير الخبرة** : يعد تقرير الخبير هو أبرز أدلة الإثبات وهو بهذه المثابة إجراء من إجراءات التحقيق ، ويلعب تقرير الخبرة الفنية دوراً بارزاً في مجال إثبات الجريمة، وعلة ذلك أنه قد تكون هناك أمور فنية تحتاج إلى خبراء أكثر تخصصاً في فحص محتويات الجهاز واسترجاع المعلومات التي تم شطبها بمعرفة المجرم المعلوماتي عقب ارتكاب جريمته ، هذا فضلاً عن أن تقرير الخبير تكون له قيمة في إثبات الجريمة باعتباره جهة محايدة ومتخصصة تخضع في النهاية لتقدير قاضي الموضوع.
- **اعتراف المتهم** : يعد الاعتراف أبرز أدلة الإثبات وبالتالي إذا اعترف المتهم بارتكاب إحدى جرائم المعلومات فلا يوجد ما يحول دون التعويل على ذلك الدليل في إثبات الجريمة ، وإن كان ذلك فرض نادر الحدوث.
- **شهادة الشهود** : يعتبر من الشهود في نطاق جرائم المعلومات الضابط القائم بالضبط وخبراء البرمجة الذين لهم دور في وضع برامج الجهاز ، مهندس التشغيل أصدقاء المتهم الذين شاهدوا واقعة بث رسائل التهديد عبر شبكة الإنترنت ، أو إرسال فيروسات للجهاز ، لا يوجد ما يمنع من التعويل على شهادتهم ، لأن تقدير هذه الشهادة موكول لمحكمة الموضوع باعتبارها من مسائل الواقع لا تخضع فيها لرقابة محكمة التمييز.

ومما سبق يتضح أن جرائم المعلومات تحتاج لإعادة صياغة النصوص العقابية بالشكل الذي يتلاءم مع الفكر العقابي الحديث لشمول أكبر قدر من الجرائم كالتجسس الصناعي والاقتصادي والعسكري عبر شبكة الإنترنت ، تنقيح النصوص التجريمية بما يكفل وضع ضوابط لجرائم المعلومات ، فمن الملاحظ أن نصوص جرائم التزوير المعلوماتي لم تتناول دعائم ومستندات الفكر المعلوماتي اتساقاً مع التشريع الفرنسي [1]. الأمر الذي يوضح مدى القصور في الاعتماد على أسلوب سد الثغرات في مكافحته ، بما يعزز من الدعوة إلى إيجاد أسلوب بديل أكثر فعالية للوقاية من جرائم المعلومات قبل وقوعها وهو ما يستلزم مزيداً من الاهتمام بالتعرف على التقنيات والآليات الجديدة بالشكل الذي يضمن عدم استغلالها في جرائم المعلومات ، وذلك بهدف تقليص حجم الخسائر الناجمة عنها قبل حدوثها.

الخلاصة

- تعرض هذا البحث لدراسة وتحليل ماهية وأشكال جرائم المعلومات في ظل التطورات المعاصرة ، حيث تناول التحليل دراسة ثلاثة نقاط رئيسية ، هي أهمية دراسة جرائم المعلومات لما لها من تأثير النواحي الاقتصادية وماهية وأشكال وخصائص جرائم المعلومات الناجمة عن تلك التطورات.
- وتناولت الدراسة بالتحليل كلاً من التقدم في تكنولوجيا المعلومات والاتصالات وعولمة الأسواق كأحد أبرز التطورات التي حدثت خلال الآونة الأخيرة. وتوصلت إلى أن تلك التطورات على الرغم مما أدت إليه من مزايا وآثار إيجابية ، إلا أنها ساعدت بشكل رئيسي في نفس الوقت على ظهور أشكال وصور جديدة من جرائم المعلومات.

[1]- تنص المادة 2/244 عقوبات فرنسي " التزوير هو تغيير تدليسي للحقيقة بسوء نية من شـــأنه الإضـــرار بالغير أياً كانت الوسيلة المتبعة في مستند مكتوب أو دعامة من دعائم الفكر التي من شأنها إثبات حق أو واقعة لها نتائج قانونية ".

- ومن خلال استعراض أبرز أشكال وصور تلك الجرائم ، اتضح أن قدراً كبيراً منها يرتبط بالاحتيال ، أو ما يعرف بجريمة أصحاب الياقات البيضاء المرتبطة بالكمبيوتر أو الإنترنت. ثم انتقل التحليل للتركيز على صور الجريمة المتمثلة في تزوير وسرقة بطاقات الائتمان والبطاقات البلاستيكية ، وتزوير المستندات الإلكترونية.
- وتوصل التحليل إلى أن جرائم المعلومات تمثل أهمية كبرى في المجتمع بعد أن ظهرت منها أنماط جديدة كالإرهاب الحاسوبي وحرب الإنترنت بالقرصنة على المواقع العسكرية وفي سبيل تحديد والوقوف على المفهوم الدقيق لجرائم المعلومات كان لابد للدراسة من التعرف على أبرز الأشكال والصور التي تتخذها هذه الجرائم في هذا المجتمع الجديد ، حيث اتضح أن هناك أشكالاً شائعة وخاصة من أبرزها الاحتيال وسرقة المعلومات ، الدخول المحظور على الحاسب الآلي وإتلاف بياناته ومحتوياته ، ونشر رسائل التهديد والصـــور الإباحية عبر الشبكة ، قطع شبكات الاتصال ، التجسس عبر الأقمار الصناعية ، التعدي على الحقوق الناشئة عن البث الإعلامي.
- ثم سعت الدراسة لإزالة الجدل القائم حول مفهوم وحدود جرائم المعلومات في المجتمع الإلكتروني ، حيث عرفت بأنها " الأفعال التي ترتكب عمداً ، أو عن طريق الامتناع على جهاز الحاسب الآلي ، أو أي موقع ، أو نظام إلكتروني ، أو شبكة اتصالات ، سواء كان ذلك النظام شبكة اتصالات دولية ، أو داخلية أو شبكة مصرفية ، أو أقماراً صناعية بهدف التعدي على الأموال المادية والمعنوية ، أو إذا وقعت الجريمة بإهمال ، ونشأ عن ذلك التعدي على الأموال المادية والمعنوية ".
- ثم سعت الدراسة أيضاً لإزالة الجدل المرتبط بالنواحي الإجرائية لجرائم المعلومات سواء من حيث القانون الواجب التطبيق في هذه الجرائم لما تتسم به من بعد دولي أحياناً، فضلاً عن حدود وسلطات جهات الاستدلال ، ضوابط الدليل المعلوماتي.
- من هنا فيمكن القول بأن أشكال جرائم المعلومات تنطوي على قدر كبير من الخطورة بالشكل الذي يستلزم مزيداً من الاهتمام بالنظر إلى أن هذه الجرائم تغير من نفسها ولا تقف عند حد معين فالتطور التكنولوجي لا يتوقف بل هو في تطور مستمر فالتقنيات ،

والطرق المستحدثة التي يمكن أن تقدمها أي خدمة إلكترونية جديدة كالتجسس عبر الأقمار الصناعية في كافة المجالات ، وإمكانيات استغلال ذلك في قتل الأبرياء والحصول على معلومات عسكرية يؤثر بشكل بالغ على كيانات الدول.

التوصيات

1- ضرورة إعادة صياغة النصوص العقابية بالشكل الذي يتلاءم مع الفكر العقابي الحديث لشمول أكبر قدر من الجرائم مثل جرائم التعدي على حقوق الشركات في البث الإعلامي عبر الأقمار الصناعية ، أو استغلال هذه الأقمار الصناعية في أغراض التجسس الصناعي والاقتصادي ، والعسكري.

2- تنقيح النصوص التجريمية بما يكفل وضع ضوابط لجرائم المعلومات ، فمن الملاحظ أن نصوص جرائم التزوير المعلوماتي لم تتناول دعائم ومستندات الفكر المعلوماتي اتساقاً مع التشريع الفرنسي.

3- ضرورة تبني الفكر الوقائي في جرائم المعلومات ، حيث أن الاعتماد على الفكر الحمائي قد ثبت أنه غير فعال وغير كافياً لمكافحة جرائم المعلومات.

4- ضرورة التزام الدول بوضع ضوابط دولية ، والتعاون الدولي لمكافحة جرائم التعدي على حقوق الشركات في البث الإعلامي عبر الأقمار الصناعية ، أو استغلال هذه الأقمار الصناعية في أغراض التجسس الصناعي والاقتصادي والعسكري لأنه بدون التعاون الدولي يصعب مكافحة هذه الجرائم.

5- ضرورة وضع ضوابط تكفل عدم قطع خدمات الإنترنت لحماية شبكات الإنترنت من تسلط بعض الدول احتراماً للبروتوكولات الدولية ، وقد أكدت ذلك المادة (32) من اتفاقية بشأن الجريمة الإلكترونية الصادرة من المجلس الأوروبي في 2004/7/1 على حق الدول في الوصول العابر للحدود إلى البيانات الكمبيوترية المخزنة بإذن أو حيث تتوفر علناً حيث يجوز لكل طرف بدون الحصول على إذن من طرف آخر.

6- ينبغي على تشريعات الدول العربية الاقتداء بالتشريع الفرنسي في المواد 5/335 عقوبات وما بعدها ، أن تدرج في تشريعاتها العقابية جرائم الإهمال في الحفاظ على بيانات الحاسب الآلي ، كإهمال الموظف في الحفاظ على الأرقام السرية ، أو المعلومات الخاصة بالجهة التي يعمل بها مما يترتب عليه تعطيل الأعمال ، أو دخول الهاكـــر على جهاز الكمبيوتر والحصول على معلومات سرية ، أو سرقة أموال العملاء ، ذلك لأن الإهمال في نطاق جرائم المعلومات أمر متصور عملاً مما يقتضي الأمر ضرورة التدخل التشريعي السريع لوضع نصوص تكفل تجريم صور الإهمال الذي يترتب عليه الدخول على نظام مجهز آلياً سواء كان حاسباً آلياً أو نظاماً محمياً إلكترونياً – أو جهاز حاسب آلي – أو شبكة مصرفية.

7- ضرورة وضع ضوابط تكفل الحماية الجنائية ضد جرائم سرقة بطاقات الائتمان ، فيتعين أن يطلب من المستخدم عند إجراء المعاملة إدخال بعض المعلومات التعريفية ، مثل الرقم السري ، الرمز البريدي ، بيانات رخصة القيادة ، العنوان ، تاريخ الميلاد ، ذلك لأنه من الملاحظ أن أماكن التسوق لا تطلب هذه البيانات ، وقد لا يكتشف المجني عليه سرقة بطاقات الائتمان إلا في وقت متأخر ، ولا يعد توقيع المستخدم دليلاً لأن سارق هذه البطاقة قد يزيلها بتوقيع ، وينسبه لمالكه الأصلي ، أما اشتراط إدخال الرقم السري عند الشراء من أماكن التسوق فإنه يحمي مالك البطاقة ، بل نذهب أبعد من ذلك بضرورة تحديث بيانات هذه البطاقات بوضع صورة شخصية للمستخدم لإمكانية تمييزه إذا اقتضى الأمر ، أو تصوير شخص القائم بالمعاملة سواء عند التسوق أو السحب لإمكانية التوصل إلى شخصيته عند وضع حد ائتماني معقول عند استخدام بطاقة الائتمان الخاصة بالإنترنت بحيث يقلل من مخاطر فقدانها والاستيلاء غير المشروع عليها وإلزام البنوك الدولية والمحلية بتطبيقه.

8- تطوير نظام آمن للتجارة الإلكترونية والذي يمنح التجار خدمة نظام دفع آمن لتمرير عمليات الشراء عبر الإنترنت ، ضرورة التدخل التشريعي بوضع نصوص تبيح للنيابة العامة حق ندب مأموري الضبط القضائي لمراقبة شبكة الإنترنت شرط أن تكون هناك

جريمة وقعت بالفعل وتأرجحت نسبتها إلى مرتكبها وأن تكون المراقبة بهدف ضبط أدلة الجريمة.

9- ضرورة إجراء دورات تدريبية مستمرة للقضاة ، وأعضاء النيابة العامة ، وخبراء وزارة العدل على مفهوم الجرائم المعلوماتية وطرق التحقيق فيها ، وكيفية استخلاص الدليل الإلكتروني ، وتثقيف الضباط القائمين على تنفيذ القانون لكيفية ضبط جرائم المعلومات واتخاذ الإجراءات التحفظية للأدلة فيها خوفاً من ضياع المعلومات ، فضلاً عن منحهم أجهزة حديثة ، ومعدات أخرى تساعدهم في كشف الأدلة في جرائم المعلومات.

10- ضرورة إنشاء محاكم متخصصة في جرائم المعلوماتية.

11- تجريم مختلف جرائم المعلومات ، وكافة جرائم الاحتيال عن طريق الكمبيوتر أو الشبكة وكل ما يكون من شأنه إلحاق أضرار غير مشروعة ، وتدمير أو تغيير أو حذف وإزالة برامج الكمبيوتر ، أو البيانات الواردة في الكمبيوتر ، أو التدخل غير المشروع في برنامج الكمبيوتر ، أو نظام الحاسوب ، أو شبكة الإنترنت.

12- إجراء تقييم لاحتياجات الدول والموارد المحلية ، بما في ذلك الموارد القضائية لاستخدامها في مجال التحقيق وتنفيذ القوانين الخاصة بجرائم المعلومات.

13- وضع خطة لتنسيق البرامج الممولة لخدمة وتنفيذ القوانين الخاصة بجرائم المعلومات ، مع توفير برامج التدريب ، مثل (برنامج تنفيذ القوانين المحلية ، والحد من جرائم المعلومات) في الولايات المتحدة الأمريكية [1].

1-Computer Crime Enforcement Act (Introduced in House Agencies To establish a grant program to assist State and local law enforcement in deterring, investigating, and prosecuting computer crimes. -IN THE HOUSE OF REPRESENTATIVES-September 8, 1999.

http://www.law.cornell.edu/search/index.html

المراجع

1- د. علاء الدين محمد فهمي ، الموسوعة الشاملة لمصطلحات الحاسب الآلي ، موسوعة دلتا كمبيوتر ، مطابع الكتاب المصري الحديثة ، 1991.

2- المستشار الدكتور. عبدالفتاح مراد ، الحكومة الإلكترونية ، مطبعة جامعة الإسكندرية.

3- د. محمد الأمين البشرى ، التحقيق في جرائم الحاسب الآلي ، مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت ، المنعقد في الفترة من أول حتى 3 مايو 2000 ، كلية الشريعة والقانون بدولة الإمارات.

4- د. هشام محمد فريد رستم ، الجرائم المعلوماتية ، أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت ، المنعقد في الفترة من 1-3 مايو 2000 ، كلية الشريعة والقانون بدولة الإمارات.

5- د. حسن عبدالباسط جميعي ، إثبات التصرفات القانونية التي تم إبرامها عن طريق الإنترنت ، دار النهضة العربية ، مصر 2000 ، الطبعة الأولى.

6- محمد حماد مهرج الهيتي ، الحماية الجنائية لبطاقات الائتمان الممغنطة ، دار الكتب القانونية ، دار شتات للنشر والبرمجيات.

7- د. محمود شريف بسيوني ، غسل الأموال وجهود المكافحة الإقليمية الوطنية ، دار الشروق ، طبعة 2004.

8- د. خالد حامد أحمد مصطفى ، جريمة غسل الأموال دراسة مقارنة ، منشأة المعارف ، طبعة 2008.

9- المستشار الدكتور. عبدالفتاح بيومي حجازي ، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت ، دار الكتب القانونية 2007.

10- د. جميل عبدالباقي الصغير ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت ، دار النهضة العربية ، طبعة 2002.

11- د. محمد محيي الدين عوض ، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة من 25 إلى 28 أكتوبر.

12- BernetRollanoe:- L Principes de technique bancaire, Paris, Dunod, 2002,

13- Strategy Report- International Narcotics Control Released by the Bureau for International Narcotics and Law Enforcement Affairs -March 2004

14- UNCTAD (2004), The E-Commerce and Development Report 2004, United Nations, New York and Geneva

15- Michael Alexander , computer crime , UGLY ,secret for business computer world vol. XXIV,NO.11.1990pp1,4
16- Report of the International High Tech Crime Investigation Association -Todd G. Shipley International President, 2010 -Carol Hutchings Executive Director The HTCIA International Executive Committee Officers
17- Federal Bureau of Investigation Retrieved 2010-08 http://www.fas.org/irp/agency/doj/fbi/2009just.pdf. "Congressional budget justification, FY 2009"and Research Centers White Collar Crime, simultaneously in Canada, United States of AmericaCopyright @ D.C. Heath and Company-1982
18- Jamie Doward (2008-03-09 .("How boom in rogue ticket websites fleeces Britons" TheObserverLondon . http://www.guardian.co.uk/world/2008/mar/09/olympicgames2008.internet . Retrieved 9 March 2008
19- Anderson, Kent (October 13, 2010). "Virtual Hostage: Cyber terrorism and politically motivated computer crime". The Prague Post. http://praguepost.com/opinion/5996-virtual-hostage.html. Retrieved 2010-10-14
20- What is cyberterrorism? Even experts can't agree. Harvard Law Record. Victoria Baranetsky. November 5, 2009.- http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA439217
21- "War is War? The utility of cyberspace operations in the contemporary operational environment" U.S. Army War College, February 2010
22- Mann, D. and Sutton, M. (1998) >>Netcrime: More Change in the Organization of Thieving. British Journal of Criminology. www.Oxfordjournals.org
23- Financial Action Task Force on Money Laundering , & Terrorist financing :- typologies reports 2005 FATF-IXhttp://www.fatf-gafi.org/pdf/TY1998_en.pdf
24- United States Attorney's Office ,Central District of California (9 August 1999). "Kevin Mitnick sentenced to nearly four years in prison; computer hacker ordered to payrestitution to victim companies whose systems were compromised" .Pressrelease . http://www.usdoj.gov/criminal/cybercrime/mitnick.htm www.lemondepolitique.fr/cours/droit_penal/general/applicatio
25- http://www.legifrance.gouv.
26- http://www.state.gov/p/inl/rls/nrcrpt/2003/vol2/html/29910.htm
27- http://en.wikipedia.org/wiki/Computer

28- http:www.orienttel.net
29- http:www.cybercrime.gov
30- www.surveillanceissues.com
31- Computer Crime Enforcement Act (Introduced in House Agencies To establish a grant program to assist State and local law enforcement in deterring, investigating, and prosecuting computer crimes. -IN THE HOUSE OF REPRESENTATIVES-September 8, 1999
http://www.law.cornell.edu/search/index.html.

Informatics & Criminal Liability [1]

Dr. Khalid Hamid Ahmed Mustafa [2]
Assistant Lecturer – Criminal Law Section - Ajman University – UAE

Abstract

The study raises the subject of information technology – related crimes as it is all inclusive of all types of intentional and unintentional Criminal behavior in the information field. In spite of using an integrated theory for analyzing information crimes and their forms, yet penal articles provided in most legislations do not tally with the modern punishment trend. The treatise sums up with narrowing down information crimes to four major kinds namely; Computer Crimes (cyber crimes), Internet Crimes, Online Banking and Satellite crimes. Spotting some hindrances as regards the body concerned for collecting evidences and investigating on such crimes, the treatise reveals a legislative conflict on the criminal behavior that leads to them. This is may be ascribable to the very nature of the crimes which are not traditional ones. Besides, the treatise reveals obstacles witnessed in the trial process in terms of crime evidence. Another point raised by the treatise is the appropriate law(local or regional or international) that should be applied on information crimes as cross- border ones which require extradition agreements. Treatise in its epilogue stresses the paramount importance of training law enforcers on the various techniques of combating Information Crimes, as well as redrafting penal articles so as to tally with the modern punishment ideology. New articles, as researcher suggests should encompass a wider range of crimes; such as infringing on the rights of Satellite broadcasting companies and military, industrial and economic satellite spying. The treatise also suggests that international rules for cooperation in combating information crimes should be laid down, and that Arab legislations should be modeled on the French ones which laid down a host of rules governing credit cards theft crimes and other information – related ones. Finally, the researcher stresses the necessity of developing safer E. Trade systems as well as forming a separate panel composing of experts and judges to decide on information – related crimes.

Keywords: Informatics – Criminal Liability – Modern Crimes – IT Crimes – Cyber Crimes – Internet Crimes – Satellite Crimes.

1-**Manuscript** was submitted in June 2011, refereed in July 2011 and approved for publication in August 2011.

2-**Biography:** Dr. Khalid Hamid was an ex- head of court and prosecuting attorney in Egypt. He wrote a book on penal procedures in UAE, besides; he contributed a host of studies for the Academy. He participated in a number of local and international conferences and debates.